

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device, the method comprising:

counting a first number of oscillations of a first oscillator on the FPGA during a predetermined time interval;

counting a second number of oscillations of a second oscillator on the FPGA during the predetermined time interval;

generating a ratio between the first number and second number of oscillations,  
wherein the ratio is generating a fingerprint that represents within the FPGA, the  
fingerprint representing an inherent manufacturing process characteristic unique to the  
FPGA, wherein generating the fingerprint includes measuring propagation delays for a  
plurality of circuit elements on the FPGA and combining the propagation delays to  
generate the fingerprint;

transmitting encrypted configuration data from the storage device to the FPGA;  
and

decrypting the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data.

2. (Original) The method of Claim 1, further comprising:  
configuring the FPGA using the configuration data.

3. (Original) The method of Claim 2, further comprising:  
transmitting the fingerprint from the FPGA to an encryption circuit;  
encrypting the configuration data using the fingerprint as an encryption key; and  
storing the encrypted configuration data in the storage device.

4. (Original) The method of Claim 1, wherein the fingerprint is generated during power-up of the FPGA.

Claims 5-6. (Cancelled)

7. (Currently Amended) The method of Claim 1 [[6]], wherein the first and second oscillators comprise comprises a configurable logic blocks block of the FPGA.

Claims 8–11. (Cancelled)

12. (Currently Amended) A field programmable gate array (FPGA), comprising:  
a plurality of configurable logic elements being programmable with configuration data to implement a desired circuit design;  
a fingerprint element for generating a fingerprint representing inherent manufacturing process variations unique to the FPGA, wherein the fingerprint element includes, ~~a plurality of circuit elements, means for measuring propagation delays for each of the plurality of circuit elements and means for combining the propagation delays to generate the fingerprint~~  
~~first and second oscillators; and~~  
~~a sensing circuit including,~~  
~~means for counting a first number of oscillations of the first oscillator and counting a second number of oscillations of the second oscillator during a predetermined time interval; and~~  
~~means for generating a fingerprint as a ratio between the first number and second number of oscillations; and~~  
a decryption circuit coupled to receive encrypted configuration data, the decryption circuit configured to decrypt the encrypted configuration data using the fingerprint as a decryption key to extract the configuration data.

13. (Original) The FPGA of Claim 12, further comprising:  
a configuration circuit for configuring the configurable logic elements with the configuration data.

Claim 14. (Cancelled)

15. (Previously Presented) The FPGA of Claim 12, wherein the configuration data is encrypted using the fingerprint as an encryption key to generate the encrypted configuration data.

Claims 16-20. (Cancelled)

21. (Currently Amended) The FPGA of Claim 12 [[20]], wherein the first and second oscillators comprise comprises a configurable logic blocks block.

Claims 22–43. (Cancelled)